What is claimed is:

Claims

1. A method comprising the steps of:

generating, by a first system device, a first encryption key;

forwarding the first encryption key from the first system device to a second system device;

storing the first encryption key at the second system device.

2. The method of claim 1, further comprising the steps of:

generating a second encryption key by combining the first encryption key with a third encryption key;

forwarding the second encryption key to a third system device.

3. The method of claim 2, wherein the third system device is any of a base station, a base site, and a TETRA site controller, wherein the step of forwarding the second encryption key to a third system device is triggered by a mobile station residing at any of the base station, the base site, and the TETRA site controller when the first encryption key is generated, and wherein the mobile station is affiliated with a talkgroup associated with the first encryption key.

4. The method of claim 2, wherein the third system device is any of a base station, a base site, and a TETRA site controller, wherein the step of forwarding the second encryption key to a third system device is triggered by a mobile station

arriving at any of the base station, the base site, and the TETRA site controller, and wherein the mobile station is affiliated with a talkgroup associated with the first encryption key.

5. The method of claim 2, wherein the third system device is any of a base station, a base site, and a TETRA site controller, wherein the step of forwarding the second encryption key to a third system device is triggered by a mobile station changing talkgroup affiliation while residing at any of the base station, the base site, and the TETRA site controller, and wherein the mobile station changes talkgroup affiliation to a talkgroup associated with the first encryption key.

6. The method of claim 2, wherein the third encryption key is associated with the third system device.

7. The method of claim 2, wherein the third encryption key is a common cipher key.

8. The method of claim 2, further comprising the step of communicating over an air interface by encrypting messages with the second encryption key.

9. The method of claim 2, further comprising the step of updating the first encryption key when an encryption period associated with the third encryption key expires.

10. The method of claim 1, further comprising the step of encrypting the first encryption key with an interkey, yielding a first encrypted encryption key;

forwarding the first encrypted encryption key to a fourth system device;

decrypting, by the fourth system device, the first encrypted encryption key into the first encryption key.

11. The method of claim 10, further comprising the steps of:

generating a second encryption key by combining the first encryption key with a third encryption key;

forwarding the second encryption key to a fifth system device.

12. The method of claim 11, wherein the second encryption key is encrypted with an intrakey prior to being forwarded to the fifth system device.

13. The method of claim 11, wherein the third encryption key is associated with the fifth system device.

14. The method of claim 11, wherein the third encryption key is a common cipher key.

15. The method of claim 1, further comprising the steps of:

encrypting the first encryption key with a key associated with a mobile station, yielding an encrypted mobile encryption key;

forwarding the encrypted mobile encryption key to the mobile station.

16. The method of claim 15, further comprising the steps of:

decrypting, by the mobile station, the encrypted mobile encryption key with the key associated with the mobile station, yielding the first encryption key;

combining the first encryption key with a predetermined encryption key, yielding an air interface key;

communicating over an air interface by encrypting messages with the air interface key.

17. The method of claim 16, wherein the predetermined encryption key is a common cipher key.

18. The method of claim 1, further comprising the step of encrypting the first encryption key with an interkey prior to the forwarding step.

19. The method of claim 1, further comprising the step of acknowledging receipt of the first encryption key.

20. The method of claim 19, wherein the step of acknowledging comprising decrypting the first encryption key, and when the first encryption key is decrypted properly, generating an acknowledgment to be forwarded via an air traffic router to the first system device.

21. The method of claim 1, wherein the second system device contains a home location register associated with the first encryption key.

22. The method of claim 1, further comprising the step of updating the first encryption key when an encryption period associated with the first encryption key expires.

23. A method comprising the steps of:

generating, by a first system device, key material;

forwarding the key material from the first system device to a second system device;

determining whether a mobile station, for which the key material is directed, is active on the system;

when the mobile station is active, forwarding the key material to a base station where the mobile station is active;

forwarding, by the base station, the key material to the mobile station.

24. The method of claim 23, further comprising the step of encrypting the key material prior to any forwarding step.

25. The method of claim 23, wherein any of a base site and a TETRA site controller takes the place of the base station.

26. The method of claim 23, wherein the key material is forwarded from the first system device to the second system device via an air traffic router.

27. The method of claim 23, wherein the second system device is a zone controller.

28. The method of claim 23, wherein the second system device is at least one of a home location register and a visited location register.

29. The method of claim 23, wherein the key material comprises a group cipher key.

30. The method of claim 23, wherein the key material comprises a static cipher key.

31. The method of claim 23, wherein the key associated with the base station comprises an intrakey.

32. The method of claim 23, further comprising the step of encrypting the key material with an interkey prior to forwarding the key material from the first system device to the second system device.

33. The method of claim 23, further comprising the step of acknowledging receipt of the key material.

34. The method of claim 33, wherein the step of acknowledging comprising decrypting the key material, and when the key material is decrypted properly, generating an acknowledgment to be forwarded via an air traffic router to the first system device.

35. The method of claim 23, wherein the second system device contains a home location register associated with the mobile station.

36. The method of claim 23, further comprising the step of updating the key material when an encryption period associated with the key material expires.

37. The method of claim 23, further comprising the steps of:

generating, by the mobile station, an first encryption key from the key material;

combining the first encryption key with a second encryption key, yielding an air interface key;

communicating over an air interface by encrypting messages with the air interface key.

38. The method of claim 37, wherein the first encryption key is a group cipher key.

39. The method of claim 37, wherein the first encryption key is a static cipher key.

40. The method of claim 37, wherein the second encryption key is a common cipher key.

41. The method of claim 37, further comprising the step of updating the air interface key when an encryption period associated with the second encryption key expires.

42. The method of claim 23, wherein the step of forwarding the key material from the first system device to a second system device comprises the steps of:

forwarding the key material from the first system device to a third system device;

forwarding the key material from the third system device to the second system device.

43. The method of claim 42, further comprising the steps of:

encrypting the first encryption key with an interkey prior to forwarding the key material from the first system device;

decrypting, by the third system device, the key material with the interkey.

44. A method comprising the steps of:

generating an encryption key at a first system device;

encrypting the encryption key with a first intrakey associated with a second system device, yielding a first encrypted encryption key;

forwarding the first encrypted encryption key to the second system device.

45. The method of claim 44, further comprising the steps of:

encrypting the encryption key with an intrakey associated with a third system device, yielding a second encrypted encryption key;

forwarding the second encrypted encryption key to the third system device.

46. The method of claim 44, wherein the step of forwarding comprises forwarding the first encrypted encryption key transparently through at least a fourth system device prior to the second system device and storing the first encrypted encryption key at the fourth system device.

47. The method of claim 46, wherein the fourth system device is a zone manager.

48. The method of claim 44, wherein the encryption key is a static cipher key that is used when at least one of dynamic air interface encryption and authentication is inoperable.

49. The method of claim 44, wherein the first system device is a key management facility.

50. The method of claim 44, further comprising the step of forwarding an acknowledgment of receipt of the encryption key to the first system device via at least a fifth system device.

51. The method of claim 50, wherein the fifth system device is an air traffic router.

52. A method comprising the steps of:

generating an encryption key at a first system device in a communication system;

forwarding the encryption key to a second system device that serves as a home location register for a mobile station;

forwarding the encryption key to the mobile station.

53. The method of claim 52, further comprising the step of determining whether the mobile station is active in the communication system prior to forwarding the encryption key to the mobile station.

54. The method of claim 52, further comprising the step of determining whether the mobile station is active in the communication system prior to forwarding the encryption key to the mobile station, and when the mobile station is not active, inhibiting forwarding of the encryption key to the mobile station.

55. The method of claim 52, wherein the encryption key is encrypted prior to being forwarded.

56. The method of claim 52, further comprising the step of sending an acknowledgment of successful receipt of the encryption key to an air traffic router via at least a zone controller

57. A method comprising the steps of:

storing, at a home location register, key material related to mobile stations associated with the home location register;

storing, at a first visited location register associated with a first site in a first zone, key material related to a first mobile station of the mobile stations associated with the home location register;

when the first mobile station roams to a second site in a second zone associated with a second visited location register, encrypting key material related to the first mobile station with an interkey, yielding encrypted key material;

forwarding the encrypted key material to the second visited location register.

58. The method of claim 57, further comprising the steps of encrypting, by the second visited location register, the key material with an intrakey, yielding

intrakey-encrypted key material, and forwarding the intrakey-encrypted key material to any of a base station and a TETRA site controller at the second site.

59. The method of claim 57, further comprising the step of, when the mobile station is active at any of a base station, a base site, and a TETRA site controller associated with the home location register, encrypting, by the first visited location register, the key material with an intrakey, yielding intrakey-encrypted key material, and forwarding the intrakey-encrypted key material to any of the base station, the base site, and the TETRA site controller associated with the home location register.

60. The method of claim 57, wherein the key material related to mobile stations registered at the first home location register is stored at least in part in encrypted form at the home location register.

61. The method of claim 36, wherein the key material is stored at least in part unencrypted at the second visited location register.

62. A method comprising the steps of:

receiving, from a mobile station at a first site in a communication system, an encrypted message;

attempting to decrypt the encrypted message;

when the attempt to decrypt has at least partially failed, requesting, from a system device in the communication system, an encryption key associated with the mobile station;

receiving the encryption key;

decrypting the encrypted message with the received encryption key.

63. The method of claim 62, further comprising the step of exchanging, with the mobile station, messages encrypted with the encryption key.

64. The method of claim 62, further comprising the step of decrypting at least an identification of the mobile station in order to identify the requested encryption key.

65. The method of claim 64, wherein the identification of the mobile station is decrypted utilizing a common cipher key.

66. The method of claim 62, further comprising the step of forwarding an acknowledgment of receipt of the encrypted message to the mobile station.

67. The method of claim 62, wherein the encryption key is encrypted by an intrakey prior to the receiving step.

68. The method of claim 62, further comprising the steps of:

forwarding the encryption key, encrypted by an interkey, from a system device at a first zone where the encryption key is stored to a system device at a second zone including the first site;

decrypting, by the system device at the second zone, the encrypted encryption key;

encrypting, by the system device at the second zone, the encryption key with an intrakey, yielding an intrakey-encrypted key;

forwarding the intrakey-encrypted key to a system device at the first site.

69. The method of claim 62, wherein the encryption key is a derived cipher key.

70. The method of claim 62, further comprising the step of combining a first encryption key with a third encryption key, yielding the encryption key.

71. The method of claim 70, wherein the encryption key is a group cipher key.

72. The method of claim 62, wherein the system device at the first site is any of a base station, a base site, and a TETRA site controller.

73. The method of claim 62, further comprising the steps of:

determining whether the encryption key associated with the mobile station is stored at a zone including the first site;

when the encryption key associated with the mobile station is not stored at a zone including the first site, determining which zone has the encryption key, yielding a target zone;

sending a request to the target zone for the encryption key associated with the mobile station;

receiving, from the target zone, the encryption key associated with the mobile station.

74. The method of claim 62, wherein the encryption key is stored at the system device at the first site until the encryption key is replaced by another encryption key.

75. The method of claim 62, wherein the encryption key is deleted from the system device at the first site after the encryption key has not been updated for a period of time greater than an expected average authentication rate in the communication system.

76. The method of claim 62, wherein the encryption key is deleted from the system device at the first site when system device at the first site is instructed to delete the encryption key.

77. The method of claim 62, wherein the encryption key is deleted after a timeout from the system device at the first site when system device at the first site is instructed to delete the encryption key.

78. The method of claim 62, wherein the encryption key is deleted from the system device at the first site after the system device at the first site is informed that the mobile station has left the first site.

79. The method of claim 62, wherein the encryption key is deleted after a timeout from the system device at the first site after the system device at the first site is informed that the mobile station has left the first site.

80. A method comprising the steps of:

when a mobile station is located at a site in a communication system, storing at the site at least one encryption key associated with a mobile station;

determining when the mobile station leaves the site;

setting a persistence timer;

when the persistence timer expires, deleting the at least one encryption key associated with a mobile station.

81. The method of claim 80, further comprising the steps of replacing the at least one encryption key with at least another encryption key and resetting the persistence timer.

82. The method of claim 80, wherein the persistence timer is set to a persistence time that is less than an expected average authentication rate in the communication system.

83. The method of claim 80, wherein the persistence timer is set to a persistence time that is based on an expected average authentication rate in the communication system.

84. The method of claim 83, wherein the expected average authentication rate is based on an average number of times a mobile station authenticates within a time period.

85. The method of claim 80, wherein the at least one encryption key is stored at the site until the at least one encryption key is replaced by at least another encryption key.

86. The method of claim 80, wherein the at least one encryption key is deleted from the site when the at least one encryption key has not been updated for a

period of time greater than an expected average authentication rate in the communication system.

87. The method of claim 80, wherein the at least one encryption key is deleted from the site when a system device at the site is instructed to delete the at least one encryption key.

88. The method of claim 80, wherein the at least one encryption key is deleted after a timeout from the site when a system device at the site is instructed to delete the at least one encryption key.

89. The method of claim 80, wherein the step of determining when the mobile station leaves the site is performed by a zone controller.

90. A method comprising the steps of:

sending, by a mobile station at a first site in a communication system, a message indicating intent to roam to a second site;

forwarding, to a system device at the second site, an encryption key associated with the mobile station;

exchanging, between the system device at the second site and the mobile station, messages encrypted with the encryption key.

91. The method of claim 90, further comprising the step of determining a delay period.

92. The method of claim 91, further comprising the step of, after the delay period, forwarding a message to the mobile station indicating approval to register at the second site.

93. The method of claim 91, wherein the delay period is based on a relationship between the first site and the second site.

94. The method of claim 91, wherein the delay period is short when the first site and the second site are from one zone in the communication system.

95. The method of claim 91, wherein the delay period is long when the first site and the second site are from different zones in the communication system.

96. The method of claim 91, wherein the delay period is determined by a zone controller for the first site.

97. The method of claim 90, wherein the encryption key is encrypted by an intrakey prior to the forwarding step.

98. The method of claim 90, wherein the step of forwarding comprises the steps of:

encrypting the encryption key with an interkey, yielding an intergroup-encrypted key;

forwarding the intergroup-encrypted key from a system device at a first zone including the first site to a system device at a second zone including the second site;

decrypting, by the system device at the second zone, the intergroup-encrypted key into the encryption key;

encrypting, by the system device at the second zone, the encryption key with an intragroup encryption key, yielding an intragroup-encrypted key;

forwarding the intragroup-encrypted key to the system device at the second site.

99. The method of claim 90, wherein the encryption key is a derived cipher key.

100. The method of claim 90, further comprising the step of combining a first encryption key with a third encryption key, yielding the encryption key.

101. The method of claim 100, wherein the encryption key is a modified group cipher key.

102. The method of claim 90, wherein the system device at the second site is any of a base station, a base site, and a TETRA site controller.

103. The method of claim 90, wherein the encryption key is stored at the system device at the second site until the encryption key is replaced by another encryption key.

104. The method of claim 90, wherein the encryption key is deleted from the system device at the second site when the encryption key has not been updated for a period of time greater than an expected average authentication rate in the communication system after the mobile station leaves the second site.

105. The method of claim 90, wherein the encryption key is deleted from the system device at the second site when system device at the second site is instructed to delete the encryption key.

106. The method of claim 90, wherein the encryption key is deleted after a timeout from the system device at the second site when system device at the second site is instructed to delete the encryption key.

107. The method of claim 90, wherein the encryption key is deleted from the system device at the second site after the system device at the second site is informed that the mobile station has left the second site.

108. The method of claim 90, wherein the encryption key is deleted after a timeout from the system device at the second site after the system device at the second site is informed that the mobile station has left the second site.

109. A method comprising the steps of:

requesting, by a mobile station, to communicate within a communication system in an encrypted manner;

determining, by a system device in the communication system, a delay period;

after the delay period has expired, forwarding a message to the mobile station indicating approval to operate.

110. The method of claim 109, wherein the delay period is determined based on a relationship between a location of the mobile station and a storage location, within the communication system, of an encryption key associated with the mobile station.

111. The method of claim 109, wherein the delay period is short when the location of the mobile station and a location of the encryption key are in one zone in the communication system.

112. The method of claim 109, wherein the delay period is short when the location of the mobile station and an expected future location of the mobile station are in one zone in the communication system.

113. The method of claim 109, wherein the delay period is long when the location of the mobile station and a destination of the encryption key are in different zones in the communication system.

114. The method of claim 109, wherein the delay period is long when the location of the mobile station and an expected future location of the mobile station are in different zones in the communication system.

115. The method of claim 109, wherein the delay period is determined by a zone controller.

116. A method comprising the steps of:

dividing a plurality of system devices into a plurality of pools;

utilizing an intrakey to encrypt messages passed between system devices in the same pool;

utilizing an interkey to encrypt messages passed between system devices of different pools.

117. The method of claim 116, wherein each of the plurality of pools comprises a mutually exclusive subset of the plurality of system devices.

118. The method of claim 116, wherein the messages comprise at least one encryption key.

119. The method of claim 116, wherein the messages comprise session authentication information.

120. The method of claim 116, wherein each different pool utilizes a different intrakey.

121. The method of claim 116, wherein only one system device from each pool utilizes the interkey.

122. The method of claim 116, wherein the plurality of system devices are part of a communication system infrastructure that provides encrypted communications.

123. The method of claim 116, wherein at least one of the plurality of system devices has its own protection key, which protection key is utilized to encrypt and decrypt any of the intrakey and the interkey for transport to any of the at least one of the plurality of system devices.

124. The method of claim 116, wherein each pool of the plurality of pools is comprised of one or more system devices that reside in a single zone of a plurality of zones in a communication system.

125. The method of claim 124, wherein the one or more system devices that reside in a single zone are comprised of at least one of a base station, base site, TETRA site controller, and a zone controller.

126. The method of claim 124, wherein only a zone controller within each of the plurality of zones stores the interkey.

127. The method of claim 116, wherein the interkey is utilized to encrypt messages passed between a system device and a key management facility.

128. The method of claim 116, wherein a message is encrypted by one of an intrakey and an interkey based on a system device to which the message is forwarded.

129. A method comprising the steps of:

storing a protection key for each of a plurality of system devices;

when transporting key material to a system device of the plurality of system devices, encrypting the key material with a protection key associated with the system device.

130. The method of claim 129, wherein the key material is a key encryption key.

131. The method of claim 129, wherein each of the plurality of system devices has its own unique protection key.

132. A method comprising the steps of:

establish an expected lifetime for an encryption key;

determining a number of storage locations for each type of system device within a communication system;

based on the expected lifetime for the encryption key and the number of storage locations, assigning the type of system device at which to store the encryption key;

storing the encryption key at a system device of the assigned type.

133. The method of claim 132, wherein the step of determining comprises determining a number of storage locations and accessibility for each type of system device within a communication system, and the step of assigning comprises, based on the expected lifetime for the encryption key and the number of storage locations and accessibility, assigning the type of system device at which to store the encryption key.

134. The method of claim 132, further comprising the step of replacing the encryption key when its expected lifetime expires.

135. The method of claim 132, wherein the encryption key is a derived cipher key that is stored at any of a base station, a base site, and a TETRA site controller.

136. The method of claim 132, wherein the encryption key is a common cipher key that is stored at any of a base station, a base site, and a TETRA site controller.

137. The method of claim 132, wherein the encryption key is a modified group cipher key that is stored at any of a base station, a base site, and a TETRA site controller.

138. The method of claim 132, wherein the encryption key is a group cipher key that is stored at at least one of a home location register and a visited location register.

139. A method comprising the steps of:

generating an encryption key for use in a first geographical area;

forwarding the encryption key to one or more base stations covering the first geographical area;

transmitting, by at least one of the one or more base stations, the encryption key to a mobile station registered at the at least one of the one or more base stations.

140. The method of claim 139, wherein any combination of one or more base sites and one or more TETRA site controllers takes the place of the one or more base stations.

141. The method of claim 139, wherein the encryption key is encrypted with an interkey prior to the forwarding step.

142. The method of claim 141, further comprising the steps of decrypting the encrypted encryption key, and encrypting the encryption key with an intrakey prior to the forwarding step.

143. The method of claim 139, wherein the encryption key is encrypted prior to the transmitting step.

144. The method of claim 143, wherein the encryption key is encrypted with a derived cipher key prior to the transmitting step.

145. The method of claim 139, further comprising the step of sending an acknowledgment of receipt of the encryption key to a key management facility.

146. The method of claim 145, further comprising the step of checking currency of the encryption key and holding off the step of sending until the encryption key is current.

147. The method of claim 145, wherein the step of sending the acknowledgment comprises sending the acknowledgment to an air traffic router via at least a zone controller.

148. The method of claim 139, further comprising the steps of generating a second encryption key for use in a second geographical area adjacent to the first geographical area, and forwarding the second encryption key to one or more base stations covering the second geographical area.

149. The method of claim 148, further comprising the step of forwarding the second encryption key to at least one of the one or more base stations covering the first geographical area.

150. The method of claim 139, further comprising the step of tracking, by the base station, currency of the encryption key.

151. The method of claim 139, wherein the encryption key is a common cipher key.

152. The method of claim 139, wherein each base station stores an encryption key associated with each geographical area adjacent to the geographical area covered by the base station.

153. A method comprising the steps of:

generating a plurality of encryption keys and associating each encryption key with one geographical area of a plurality of geographical areas;

forwarding each encryption key to one or more base stations in the geographical area associated with the encryption key;

determining at least one of the plurality of geographical areas that is adjacent to a first geographical area, yielding one or more adjacent geographical areas;

forwarding an encryption key for at least one of the one or more adjacent geographical areas to at least one base station covering the first geographical area.

154. The method of claim 153, wherein any combination of one or more base sites and one or more TETRA site controllers takes the place of the one or more base stations.

155. The method of claim 153, further comprising the step of transmitting, by at least one of the one or more base stations, the encryption key to a mobile station registered at the at least one of the one or more base stations.

156. The method of claim 155, wherein each encryption key is encrypted with at least one of an interkey and an interkey prior to the forwarding step.

157. The method of claim 156, further comprising the steps of decrypting the encrypted encryption key, and encrypting the encryption key with an intrakey prior to the forwarding step.

158. The method of claim 153, wherein each encryption key is encrypted prior to the transmitting step.

159. The method of claim 158, wherein each encryption key is encrypted with a derived cipher key prior to the transmitting step.

160. The method of claim 153, further comprising the step of sending an acknowledgment of receipt of the encryption key to a key management facility.

161. The method of claim 160, wherein the step of sending the acknowledgment comprises sending the acknowledgment to an air traffic router via at least a zone controller.

162. The method of claim 153, further comprising the step of tracking, by a base station, currency of the encryption key.

163. The method of claim 153, wherein the encryption key is a common cipher key.

164. The method of claim 153, wherein each base station stores an encryption key associated with each geographical area adjacent to the geographical area covered by the base station.